

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

**DECLARATION OF ANDREW W. APPEL IN SUPPORT OF THE
UNSEALING OF THE 2021 HALDERMAN REPORT**

I, ANDREW W. APPEL, declare, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I have over 40 years' experience in computer science, and 18 years' experience studying voting machines and elections.

2. I am the Eugene Higgins Professor of Computer Science at Princeton University, where I have been on the faculty since 1986 and served as Department Chair from 2009-2015. I have also served as Director of Undergraduate Studies, Director of Graduate Studies, and Associate Chair in that department. I have served as Editor in Chief of ACM Transactions on Programming Languages and Systems, the leading journal in my field. In 1998 I was elected a Fellow of the Association for Computing Machinery, the leading scientific and professional

society in Computer Science.

3. I received an A.B. (1981) from Princeton University summa cum laude in Physics, and a PhD (1985) from Carnegie Mellon University in Computer Science.

4. I have taught undergraduate and graduate courses at Princeton University in programming, programming languages, software engineering, election machinery, software verification, and formal methods.

5. I have testified on election technology before the U.S. House of Representatives (subcommittee on information technology, 2016), the New Jersey legislature (several committees, on several occasions 2005-2018), the Superior Court of New Jersey (Mercer County, 2009; Cumberland County, 2011), the New York State Board of Elections (2019), the Freeholders of Mercer County (2017 and 2019) and Essex County (2019).

6. I have published over 140 scientific articles and books, including many papers on computer security and several papers on voting machines, election technology, and election audits.

7. I have served as a peer-review referee for the Usenix Electronic Voting Technology workshop.

8. I am not being compensated for my work related to this matter. I expect that my expenses, if any, will be reimbursed.

9. The report on security flaws in Dominion voting machines, written by Professors J. Alex Halderman and Drew Springall in July 2021 and placed under seal by the Federal District Court for the Northern District of Georgia, should be immediately unsealed by the Court and be made public.

10. I have not read Professor Halderman's report, since it is still under seal, but (from all descriptions of it) it is a classic example of a security-vulnerability report that should now be released to the public. The report has been available to the vendor for over 500 days, so there has been ample time to patch those vulnerabilities that can be patched. In fact, Dominion claims to have fixed some vulnerabilities apparently related to the Halderman report, in their Democracy Suite 5.17 product, according to their recent filing with the EAC.

11. Today, the customers of Dominion's product—election administrators, public officials, and voters—need full information about its security so they can make their own fully informed judgments about how to run their elections. With public awareness of the vulnerabilities described in the report, citizens can then ask their state election officials to install Dominion's update rather than leaving it on the shelf.

12. Computer security experts in both industry and academia widely recognize that keeping vulnerability details secret, past the time in which a technology vendor could reasonably have patched them, harms the security of that

technology's users.

13. Vulnerabilities in computer software can be exploitable, meaning that hackers who know about these bugs can exploit them to take unauthorized actions. When such vulnerabilities persist without being fixed (“patched” in the language of computer security) and without the distribution of software updates incorporating such fixes, then users of such software suffer harms due to the insecure software. Today, it is uniformly recognized that keeping vulnerabilities secret does not provide security. If someone can discover a vulnerability, others can as well.

14. In the early decades of computer systems, vendors were very slow to patch systems. To address this problem, a system of responsible disclosure was developed in the late 1990s and early 2000s, and this system is now widely accepted by industry (both the vendors and users of software), government agencies such as CISA, and by security researchers world-wide.

15. Upon discovering a security flaw, a security researcher practicing responsible disclosure will notify the maker (either directly or via one of the organizations that exists for this purpose) of all the details needed to understand and reproduce the problem. The researcher will inform the maker that after a set period (generally around 90 days) all the details will be published.

16. The purpose of the (delayed) public disclosure is twofold:

1) to incentivize software vendors to fix their bugs and distribute those fixes

promptly (or to produce less buggy software in the first place) and 2) to inform consumers of software so that they may improve their own security, either by installing such fixes or by discontinuing the use of vulnerable software.

17. This process—early notification to vendors followed by public disclosure after a set period—is the industry norm. Corporate CSOs (Chief Security Officers) who are consumers of commercial software rely on public notification to secure their own businesses. Makers of software (at sufficiently high level of professionalism) are well-organized enough to act upon vulnerabilities disclosed to them. Google’s “Project Zero” is a team of security researchers that have released 1791 disclosures after a 90-day delay, and 6 disclosures on which they delayed release for not more than 216 days. An entire industry exists to assist companies in paying cash bounties to independent researchers who responsibly disclose bugs and vulnerabilities.

18. Before responsible disclosure, including (delayed) full disclosure of vulnerability details, became the norm, vendors would ignore security flaws and claim that the flaws were merely “theoretical.” They would leave their systems vulnerable—sometimes taking years to patch their software, or never patching their software—relying on the ignorance of their customers.

19. Those who argue that publishing vulnerabilities enables bad people to do bad things, are ignoring the fact that if one person can discover a flaw, so can

others. This is why responsible disclosure, including delayed, full disclosure, is so widely practiced and accepted in the computer and software industry.

20. In this particular case, the report in question has been widely distributed with and without authorization. Bad actors undoubtedly already have access to the report. There is further danger that it could leak to the general public at any time. A leak close to November 2024 could be used as a political tool to undermine confidence in the election.


21. For the foregoing reasons the report should be unsealed and made public.

22. Whether or not this report is unsealed, it is entirely unsafe to assume that there are no more bugs or security flaws in the Dominion software other than the ones that Professors Halderman and Springall identified for this court. Computer software (including voting-machine software) is ever more complex. As I follow reports of security vulnerabilities found in widely used software products, I see more bugs reported every year in the same products. Some of these flaws survive for years in these products before being reported. It is entirely likely that even if Dominion's modifications (for which they recently applied for EAC certification) successfully repair these specific security flaws, there are others latent in their product as well.

23. The solution is not to replace Dominion's BMDs with some other

brand of BMDs—Dominion’s competitors’ products will also have security flaws. The solution is to conduct elections in such a way that software security flaws will not lead to altered election outcomes. One such way is for voters to mark optical-scan paper ballots with a pen, and tally the ballots with optical-scan voting machines. Even if those voting machines have security flaws—as they inevitably will—we can be sure that marks on the paper ballots were not placed there by cheating software. Therefore, recounts or audits (conducted by human eyes) will not need to rely on (unattainable) perfect software security. This is not the case with Ballot Marking Devices.

24. I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 12th day of May, 2023, in Princeton, New Jersey.



ANDREW W. APPEL